CITY COUNCIL
AGENDA REPORT

SUBJECT: Adopt the "Red Flag" Identity Theft Prevention Program

AGENDA DATE: October 21, 2008

PREPARED BY: Judith Hashem, Finance Director

APPROVED FOR AGENDA BY: Ralph G. Velez, City Manager

RECOMMENDATION: City Council is requested to take the following action:

1. **Adopt the attached Resolution No. ____ adopting the "Red Flag" Identity Theft Prevention Program.**

FISCAL IMPACT: N/A

BACKGROUND INFORMATION:

The Federal Trade Commission (FTC) has adopted regulations that require "creditors", which includes municipalities that provide retail water service to customers, to develop and implement an identity theft prevention program by November 1, 2008 to comply with the Act. The City holds payment account information for customers in order to bill and collect water, wastewater and refuse services rendered.

The City is required to establish a program to maintain identifying information in order to validate the customer, to secure customer information, to identify warning signals or possible "Red Flags" of suspicious activity related to a customer account, to adopt procedures to respond to "Red Flags", to provide staff training on the program, and to review periodically for any changes needed to the program.

The program will be administered by the Finance Director and will require training of all staff members, who are designated as those positions, potentially having access to confidential customer account information in the performance of their job duties.

The City Council must adopt the "Red Flag" Identity Theft Prevention Program by Resolution.

RESOLUTION NO. ____

A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF CALEXICO ADOPTING THE "RED FLAG" IDENTITY THEFT PREVENTION PROGRAM

WHEREAS, the Federal Trade Commission (FTC) has adopted regulations that require "creditors" holding consumer or other "covered accounts", defined to mean any account where customer payment information is collected in order to bill for services rendered, to develop and implement an identity theft prevention program that complies with those regulations by November 1, 2008; and

WHEREAS, the City of Calexico provides retail water service to its customers, the City is a "creditor" under the applicable FTC regulations and therefore must comply with those regulations by adopting and implementing an identity theft prevention program; and

WHEREAS, the City recognizes that it must take action to comply with the applicable FTC regulations by adopting an identity theft prevention program.

NOW, THEREFORE, THE CITY COUNCIL OF THE CITY OF CALEXICO, CALIFORNIA, DOES RESOLVE AS FOLLOWS:

SECTION 1. Program Goals. The City of Calexico Identity Theft Prevention Program (the "program") shall endeavor to achieve the following goals:

a) To identify relevant patterns, practices, and specific activities (referred to in this program as "Red Flags") that signal possible identity theft relating to information maintained in the City's customers' accounts, both those currently existing and those accounts to be established in the future;
b) To detect "Red Flags" after the program has been implemented;
c) To respond promptly and appropriately to detected "Red Flags" to prevent or mitigate identity theft relating to City customer account information; and
d) To ensure the program is updated periodically to reflect any necessary changes.

SECTION 2. The Program.

a) The City shall assess the security of its current customer account system, with an emphasis on assessing the methods by which it opens and maintains customer accounts and customers' personal information, and on assessing the manner in which it provides access to customer accounts. That assessment shall include an analysis of any prior incidents of identity theft which the City has experienced.
b) The City shall maintain identifying information (address, social security number, etc.) for each customer so it can authenticate customers, monitor transactions, and verify the validity of customer requests, such as a change of address or service-related requests, including requests to terminate service.
c) The City shall establish a reporting system which allows the City staff to discover potential "Red Flags" as they arise and to thereafter report them to the proper authorities, including law enforcement. The reporting system shall

specifically focus on the following "Red Flags": alerts, notifications, or other warnings received from consumer reporting agencies or service providers; presentation of suspicious documents by a purported customer; presentation of suspicious personal identifying information by a purported customer, such as a specific address change; the unusual use of, or other suspicious activity related to, a customer's account; and notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with the City's customer accounts.

d) The City shall adopt procedures which provide for appropriate responses to any detected "Red Flags" which are commensurate with the degree of risk posed. In determining an appropriate response, the City shall consider aggravating factors that may heighten the risk of identity theft, such as a date security incident that results in unauthorized access to a customer's account records or notice that a customer has provided information related to a customer's account to someone fraudulently claiming to represent the City. Appropriate responses include the following: i) monitoring customer accounts for evidence of identity theft, ii) contacting the customer, iii) changing from time to time any passwords, security codes, or other security devices that permit access to customer accounts, iv) reopening a customer account with a new account, vii) notifying law enforcement, and viii) determining that no response is warranted under the particular circumstances. Any "Red Flags" shall be brought to the Finance Director's attention to determine the appropriate response(s) to be implemented promptly after detection.

e) The Finance Director of the City of Calexico, or designee, shall implement and administer the program. The Finance Director shall provide periodic reports to the City Council on the effectiveness of the program and shall ensure that all necessary City employees are properly trained to implement the program.

f) The Finance Director shall annually review the program with appropriate City staff to determine if any revisions are needed. That review may include changes in identity theft methods and changes in methods to detect, prevent, and mitigate identity theft. The Finance Director is hereby authorized and directed to recommend any changes in the program that are found to be necessary. Amendments to the adopted "Red Flag" Identity Theft Prevention Program shall be approved by the City Council.

PASSED, APPROVED AND ADOPTED THIS 21ST DAY OF OCTOBER, 2008.

_____

LOUIS FUENTES, MAYOR

ATTEST:

_____
LOURDES CORDOVA, CITY CLERK

APPROVED AS TO FORM:

_____
JENNIFER M. LYON, CITY ATTORNEY

STATE OF CALIFORNIA)
COUNTY OF IMPERIAL) SS.
CITY OF CALEXICO)

I, LOURDES CORDOVA, CITY CLERK OF THE CITY OF CALEXICO, DO HEREBY CERTIFY THAT THE ABOVE AND FOREGOING RESOLUTION NO. ____ WAS DULY PASSED AND ADOPTED BY THE CITY COUNCIL OF THE CITY OF CALEXICO ON THIS 21ST DAY OF OCTOBER, 2008 BY THE FOLLOWING VOTE, TO-WIT:

AYES:
NOES:
ABSENT:

_____
LOURDES CORDOVA, CITY CLERK

S E A L

ISSUE DATE: OCTOBER 21, 2008

Purpose

The "Identity Theft Prevention Program" is created in order to comply with regulations issued by the Federal Trade Commission (FTC), as part of the implementation of the Fair and Accurate Credit Transaction (FACT) Act of 2003. The FACT Act requires that financial institutions and creditors implement written programs which provide for detection of and response to specific activities ("Red Flags") that could be related to identity theft. The program must be in place by November 1, 2008 and must contain reasonable policies and procedures based on size, complexity and nature of the operation. The FTC regulations require that the program must:

1. Identify relevant "Red Flags" and incorporate them into the program;
2. Identify ways to detect "Red Flags";
3. Include appropriate responses to "Red Flags";
4. Address new and changing risks through periodic program updates; and
5. Include a process for administration and oversight of the program.

Definitions

The "Red Flag" rules define a "Red Flag" as a pattern, practice, or specific activity that indicates the possible existence of identity theft and "Identity Theft" as fraud committed using the indentifying information of another person.

According to the rule, the City of Calexico's municipal water/wastewater utility is a creditor subject to the rule requirements. Where non-profit and government entities defer payment for goods or services, they are considered creditors.

All City utility accounts, that are individual utility service accounts, whether residential, commercial, or industrial are covered by the rule. Under the rule, a "covered account" is:

1. Any account the City offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions; and
2. Any other account the City offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the City from identity theft.

"Identifying information" is defined under the rule as any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including name, address, telephone number, social security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, unique electronic identification number, computer's internet protocol address, or routing code.

Identification of "Red Flags"

"Red Flags" are warning signs or activities that alert a creditor to potential identity theft. The guidelines published by the FTC include 26 examples of red flags, which fall into the five categories below:

A. Alerts, notifications, or other warnings received from consumer reporting agencies or service providers.

Red Flags:

1. Report of fraud accompanying a credit report;
2. Notice or report from a credit agency of a credit freeze on a customer or applicant;
3. Notice or report from a credit agency of an active duty alert for an applicant;
4. Indication from a credit report of activity that is inconsistent with a customer's usual pattern of activity; and
5. The social security number (SSN) is invalid.

B. Suspicious documents and activities.

Red Flags:

1. Identification document or card that appears to be forged, altered or inauthentic;
2. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
3. The customer refuses to provide required identification documents when attempting to establish a utility account;
4. Other document with information that is not consistent with existing customer information (such as if a person's signature on a check appears forged);
5. A customer refuses to provide proof of identity when discussing an established utility account;
6. A person other than the account holder or co-applicant requests information or asks to make changes to an established utility account; and
7. Application for service that appears to have been altered or forged.

C. Suspicious personal identifying information.

Red Flags:

1. Identifying information presented that is inconsistent with other information the customer provides (i.e. inconsistent birth dates);
2. Identifying information presented that is inconsistent with other sources of information (i.e. an address not matching an address on a credit report);
3. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
4. Identifying information presented that is consistent with fraudulent activity (i.e. an invalid phone number or fictitious billing address);
5. Social security number presented that is the same as one given by another customer;
6. An address or phone number presented that is the same as that of another person;
7. A person fails to provide complete personal identifying information on an application when reminded to do so (note: by law social security numbers may be requested, but must not be required); or
8. A person's identifying information is not consistent with the information that is on file for the customer.

- Suspicious activity related to a covered account.

Red Flags:

1. Change of address for an account followed by a request to change the account holder's name;
2. Payments stop on an otherwise consistently up-to-date account;

3. Account used in a way that is not consistent with prior use (i.e. very high activity);
4. Mail sent to the account holder is repeatedly returned as undeliverable;
5. Notice to the utility that a customer is not receiving mail sent by the City;
6. Notice to the utility that an account has unauthorized activity;
7. Breach in the utility's computer system security; and
8. Unauthorized access to or use of customer account information.

- Notice from others.
  Red Flag:
  1. Notice to the Utility from a customer, identity theft victim, law enforcement or other person that it has opened or is maintaining a fraudulent account for a person engaged in identify theft.

Detecting Red Flags

A. New Accounts
In order to detect any of the "Red Flags" identified above associated with the opening of a new account, City Customer Service personnel will take the following steps to obtain and verify the identity of the person opening the account:
Detect:
1. Require certain identifying information such as name, date of birth, residential or business address, principal place of business for an entity, driver's license or other identification;
2. Verify the customer's identity (i.e. review a driver's license or other identification card);
3. Review documentation showing the existence of a business entity; and
4. Independently contact the customer.

B. Existing Accounts
In order to detect any of the "Red Flags" identified above for an existing account, City's Customer Service personnel will take the following steps to monitor transactions with an account:
Detect:
1. Verify the identification of customers, if they request information in person, via telephone, via facsimile, or via email;
2. Verify the validity of requests to change billing addresses; and
3. Verify changes in banking information given for billing and payment purposes.

Preventing and Mitigating Identity Theft

In the event City's Customer Service personnel detect any identified "Red Flags", such personnel shall take one or more of the following steps, depending on the degree of risk posed by the "Red Flag".

Prevent and Mitigate:
1. Continue to monitor an account for evidence of identity theft;
2. Contact the customer;
3. Change any passwords or other security devices that permit access to accounts;
4. Not open a new account;
5. Close an existing account;
6. Reopen an account with a new number;

7. Notify the Program Administrator for determination of the appropriate step(s) to take;
8. Notify law enforcement; or
9. Determine that no response is warranted under the particular circumstances.

Protect customer identifying information:
In order to further prevent the likelihood of identity theft occurring with respect to utility accounts, the City's Customer Service personnel will take the following steps with respect to its internal operating procedures to protect customer identifying information:

1. Ensure that its website is secure or provide clear notice that the website is not secure;
2. Ensure complete and secure destruction of paper documents and computer files containing customer information;
3. Ensure that office computers are password protected and that computer screens lock after a set period of time;
4. Keep offices clear of papers containing customer information;
5. Request only the last 4 digits of social security numbers;
6. Ensure computer virus protection is up to date; and
7. Require and keep only the kinds of customer information that are necessary for utility purposes.

Program Updates
This program will periodically be reviewed and updated to reflect changes in risks to customers and the security of the City from identity theft. At least (1) time per year the Finance Director will consider the City's experience with identity theft, changes in identity theft methods, changes in identity theft detection and prevention methods, changes in types of accounts the City maintains and changes in the City's business arrangements with other entities. After considering these factors, the Finance Director will determine whether changes to the program, including the listing of "Red Flags" are warranted. If warranted, the Finance Director will update the program or present the City Council with his or her recommended changes and the City Council will make a determination of whether to accept, modify or reject those changes to the program.

Program Administration and Oversight

A. Administration
Finance staff shall be responsible for implementing the program and shall be trained by or under the direction of the Finance Director in the detection of "Red Flags" and the responsive steps to be taken when a "Red Flag" is detected.

The Finance Director or designee shall be responsible to oversee the daily activities related to identity theft detection and prevention, and ensure that all staff members of the Customer Service Division are trained to detect and respond to "Red Flags". Utility staff shall provide reports to the Finance Director or designee on incidents of identity theft.

B. Oversight
Responsibility for developing, implementing and updating this program lies with the Finance Department. The Finance Department is required to prepare an annual report which addresses the effectiveness of the program, documents significant incidents

involving identity theft and related responses, provides updates related to external service providers, and includes recommendations for material changes to the program.

The program will be reviewed at least annually and updated as needed based on the following events:

- Experience with identity theft
- Changes to the types of accounts and/or programs offered
- Implementation of new systems and/or new vendor contracts

C. Service Provider Arrangements
The City of Calexico presently engages service providers to perform the services of a pay station in connection with the City utility accounts. The service providers will take the following steps to ensure activities of the pay station perform in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

1. Require, by contract, that service providers have such policies and procedures in place; and
2. Require, by contract, that service providers review the City's Identity Theft Prevention Program and report any "Red Flags" to the Finance Director.

D. Specific Program Elements and Confidentiality
For the effectiveness of the identity theft prevention program, the "Red Flag" rule anticipates a degree of confidentiality regarding the City's specific practices relating to identity theft detection, prevention and mitigation. Therefore, under this program, knowledge of such specific practices is to be limited to the Finance Director and those employees who need to know them for purposes of preventing identity theft. The program, however, is to be adopted by the City Council and publicly available.